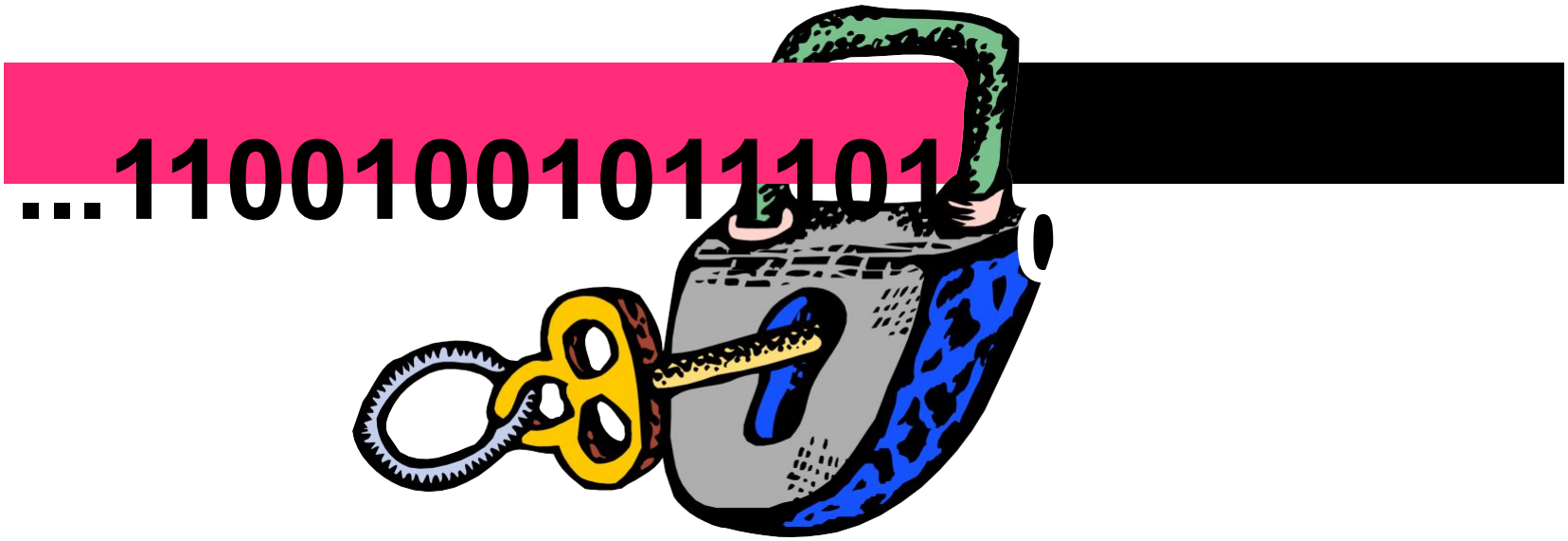
Мережева безпека



Ключові принципи, застосовні до даних у русі

Перелік тем

- **Основи кібербезпеки**
  - **Тріада CIA**
  - **Рівняння ризику**
  - **Кіберматриця**
  - **Моделі атак**
- **Представлення даних і математика обчислень**
  - **Термінологія**
  - **Системи числення**
  - **Булева логіка**
  - **Порозрядне маскування**

Тріада CIA

- **Під терміном «тріада CIA» розуміють три ключові цілі інформаційної безпеки. В основі кожного аспекту кібербезпеки лежить прагнення досягнути/виконати ці три цілі.**
  - **Конфіденційність (C — confidentiality): забезпечення того, що інформація не буде розголошена невповноваженим особам чи не стане доступною для несанкціонованих процесів чи пристроїв.**
  - **Цілісність (I — integrity): захист інформації від неналежного змінення, зокрема забезпечення її автентичності**
  - **Доступність (A — availability): своєчасний і надійний доступ до даних та інформаційних служб для вповноважених користувачів**

Загрози для «тріади CIA»

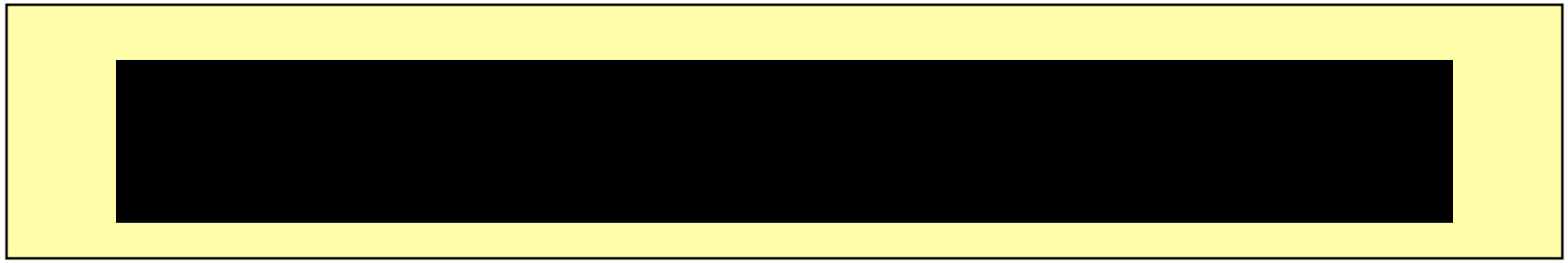
Ось речі, вбезпечити від яких прагнуть спеціалісти з інформаційної безпеки (ІБ). Серйозність будь-якої з цих загроз залежить від «критичності» інформації, на яку вона спрямована.

Зверніть увагу на значущість обох аспектів цілісності (зміна та джерело) з точки зору загрози.

- **Конфіден** Несанкціоноване **розкриття** **не буде розголош доступною для несанкціонованих процесів чи пристроїв.**
- **Цілісність: захист інформації від ненадежного змінення, зокрема урахування безвідмовності (non-repudiation) і захисту від знищення)** Несанкціоноване **змінення або уособлення**
- **Доступ** **Відмова в обслуговуванні (DoS)** **інформаційних служб для вповноважених користувачів.**

Рівняння ризику

- **Рівняння ризику дає дуже узагальнену, високорівневу картину.**
- **Рівняння має такий вигляд:**



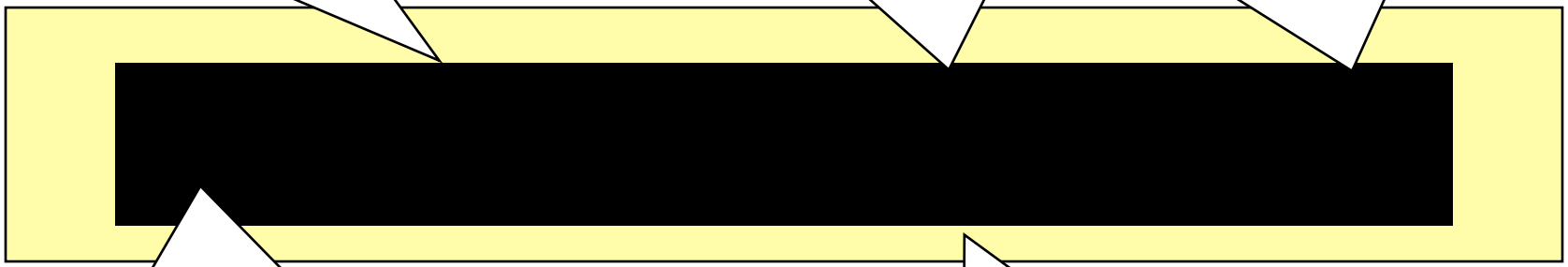
- **Примітка: добуток трьох множників у чисельнику представляє вихідний ризик.**
- **Примітка: Security_Controls («заходи з безпеки») ще часто називають «запобіжними заходами» чи «контрзаходами».**

Робота з рівнянням ризику

Захисник практично не має прямого контролю над цим. Здебільшого контролюється правовими методами знеохочення.

Атрибути структури системи (чи людської діяльності!), які зумовлюють потенціал для зумисного створення проблем чи їх випадкового виникнення.

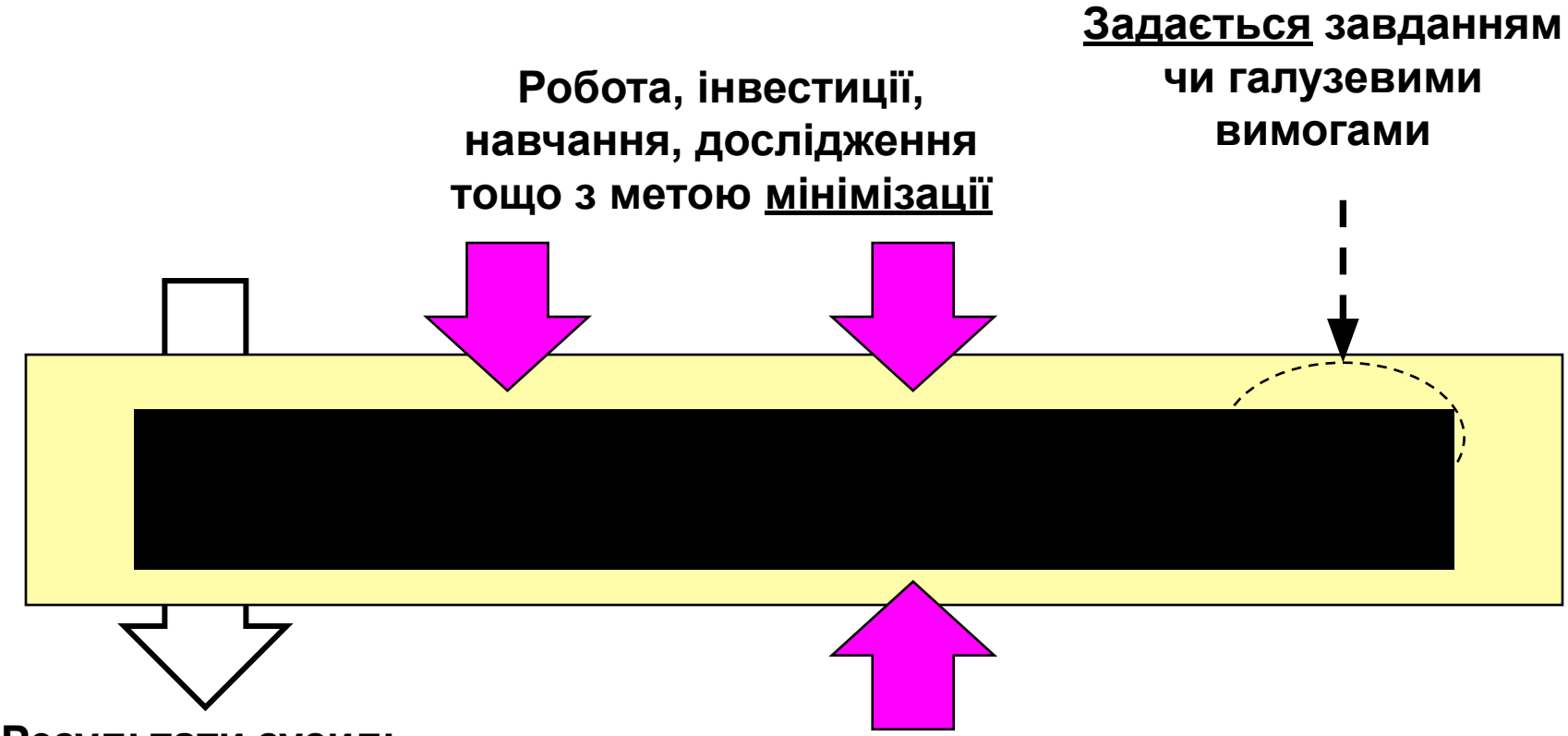
Наскільки все буде погано у випадку відмови чи атаки? Уявіть, що кожен елемент «тріади CIA» стосується грошей, довіри, готовності до виконання завдань, конкуренції тощо.



Завдання спеціаліста з ІБ полягає у зменшенні його до «прийнятного рівня». В цьому полягає вся суть сертифікації та акредитації інженерів з безпеки взагалі.

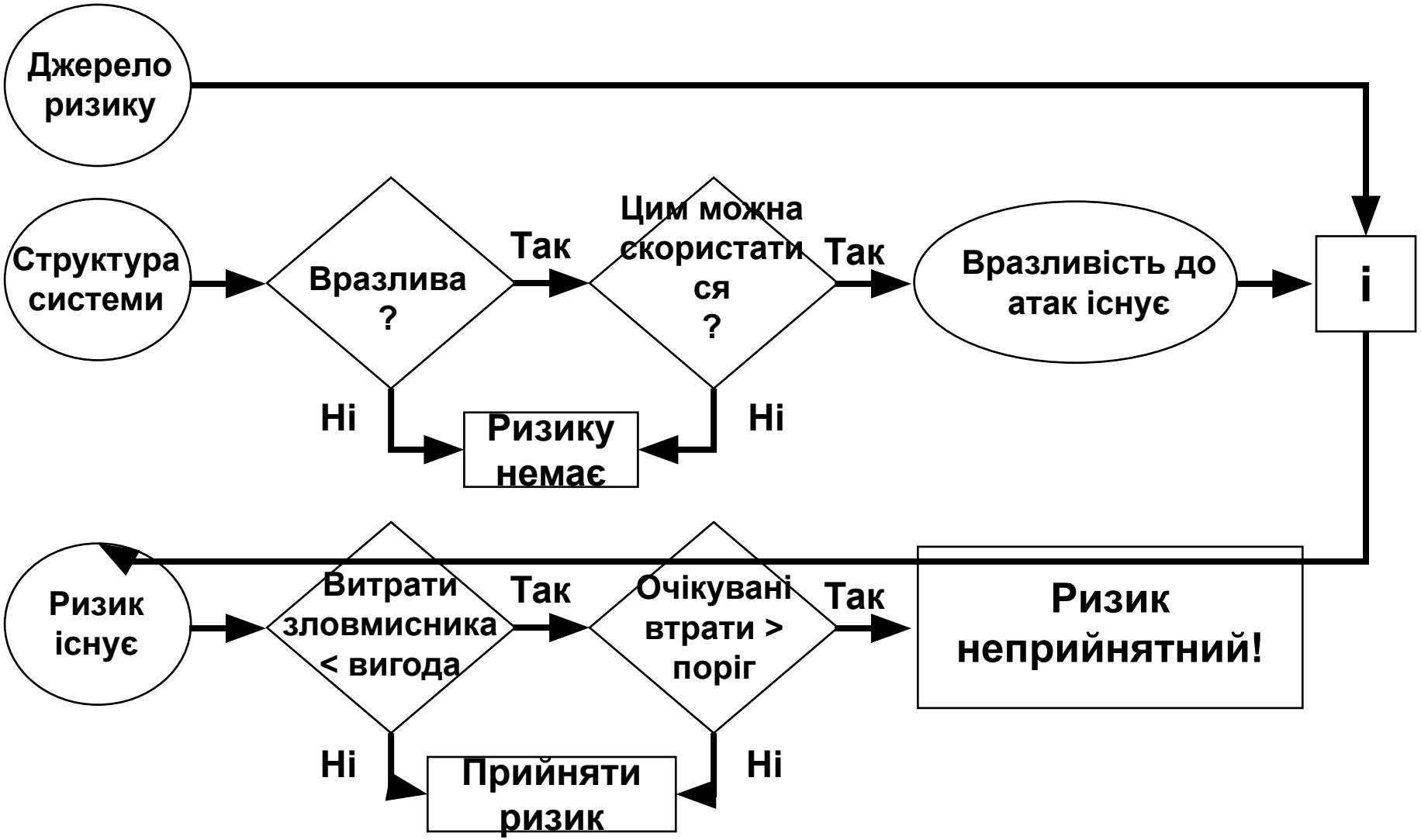
Впровадження політик, операцій, процедур, пристроїв тощо та керування ними з метою зниження ризику.

Робота з рівнянням ризику



Якби ви були в галузі кібербезпеки…
Ви б *це* робили?

Блок-схема оцінювання ризику NIST

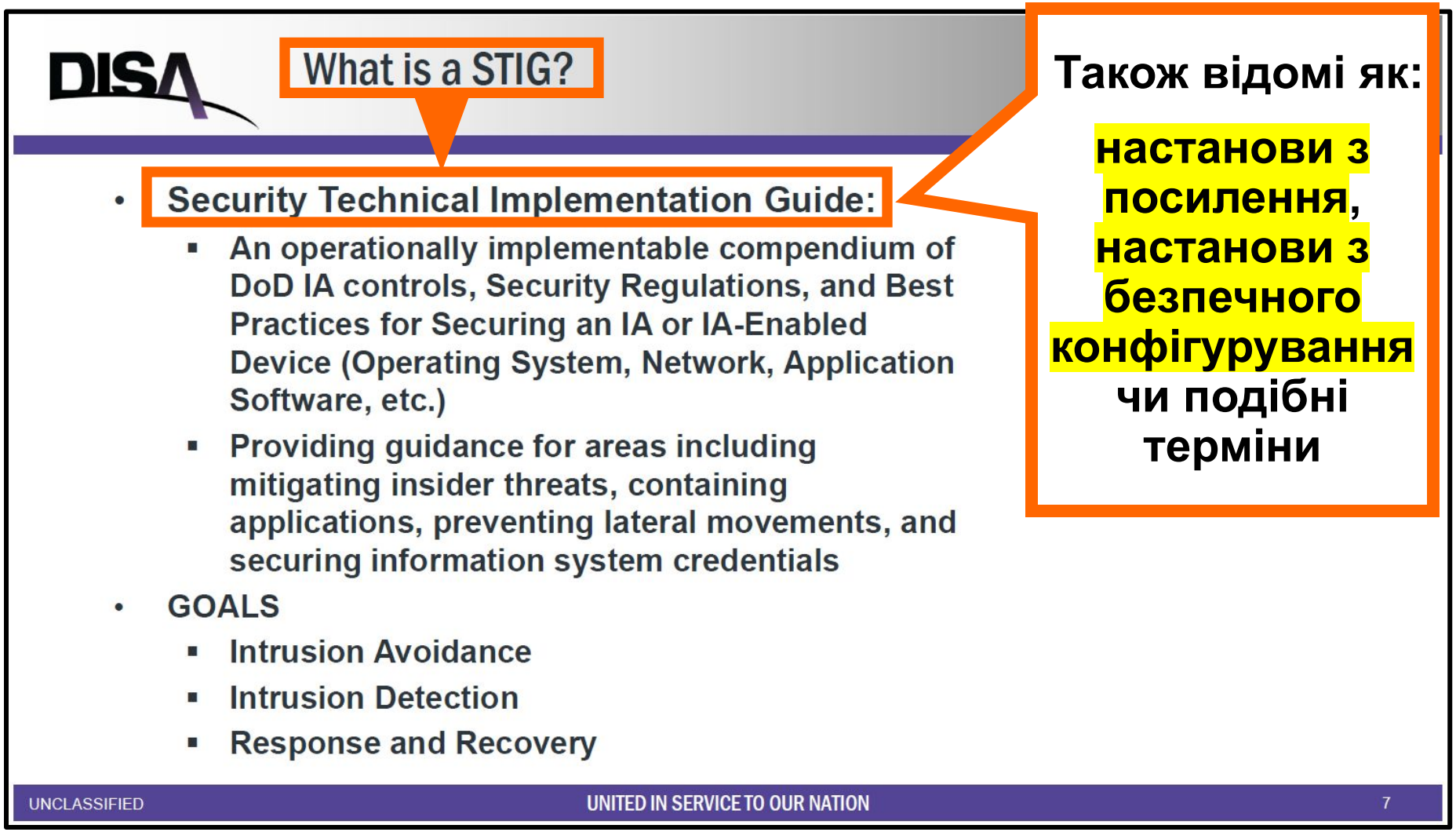


Джерело: NIST **SP800-30** «Настанови з проведення оцінювань ризиків»

Робота з рівнянням ризику

- **Зменшення вразливості** 
  - **Будуйте від початку безпечні системи!**
  - **Застосовуйте виправлення якомога скоріше.**
  - **Дотримуйтесь «POLP», тобто принципу _____ _____, наскільки це можливо**
  - **Дотримуйтесь «STIG» (див. наступний слайд)**
- **Максимізація «Security_Control»** 
  - **Визначайте й отримуйте якісні безпекові продукти.**
  - **Забезпечте правильне встановлення, конфігурування та впровадження.**
  - **Прагніть побудувати/застосовуйте ешелонований захист.**
- **Зберігайте «раціональну параною».**

Слайд 7 з «Security Standards: Getting the Protections in Place», McKinney (DISA) від 21 квітня 2016 року



Слайд 20 з «Security Standards: Getting the Protections in Place», McKinney (DISA) від 21 квітня 2016 року

UNCLASSIFIED

DISA

STIG Impacts

- Internal analysis has shown over [redacted] of cyber incidents could have been prevented if STIGS were applied
- Rapid response to real-time cyber attacks
- Industry and government can benefit from security standards

Маєте здогадки щодо цього відсотка?

STIG Support Help Desk disa.stig_spt@mail.mil

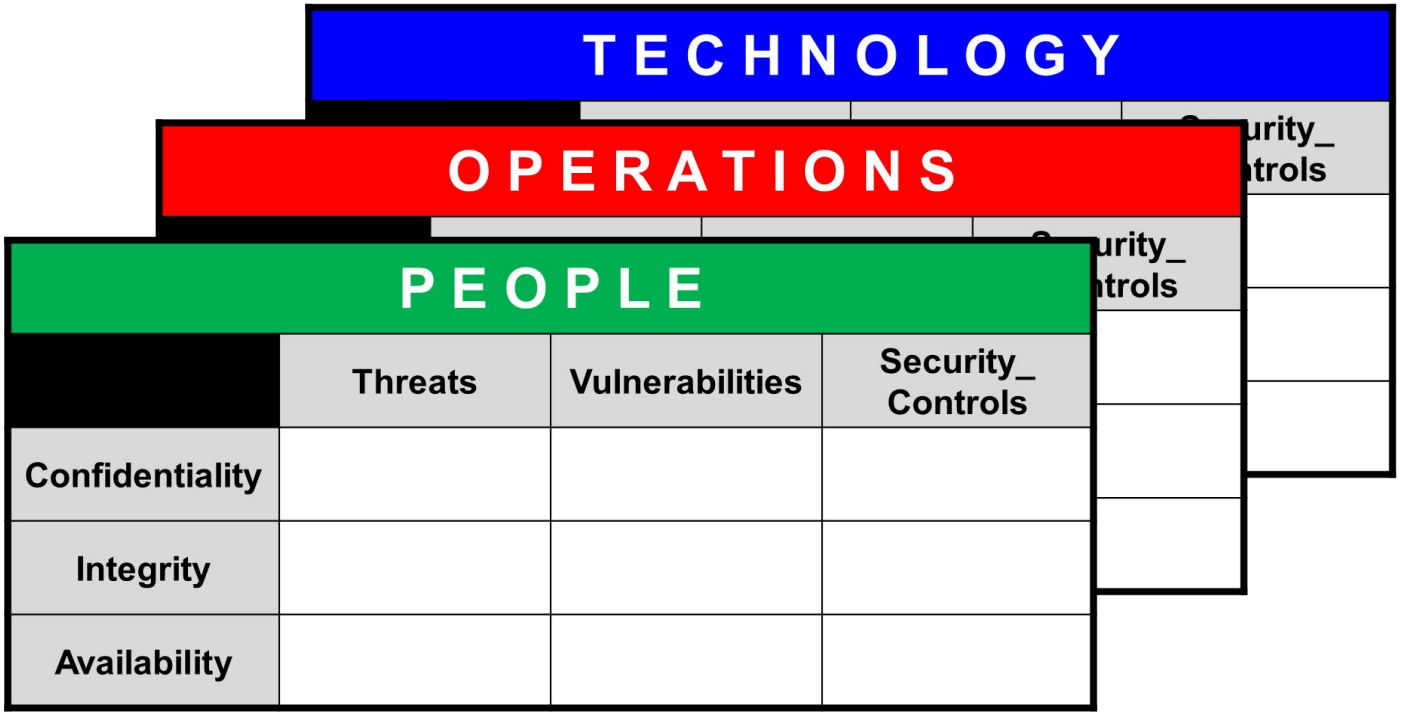
Кібератриця

	Загрози	Вразливості	Заходи з безпеки
Конфіденційність			
Цілісність			
Доступність			

Поєднання «*тріади CIA*» (тобто трьох цілей інформаційної безпеки) із контрольованими параметрами рівняння ризику дає кібератрицю.

Кіберматриця

Розгляд «тріади CIA» з точки зору людей, операцій і технології і поєднання її з контрольованими параметрами рівняння ризику дає кіберматрицю 3 × 3 × 3. Суть цієї матриці полягає в її можливості широкого охоплення всіх елементів кібербезпеки у зрозумілій формі.



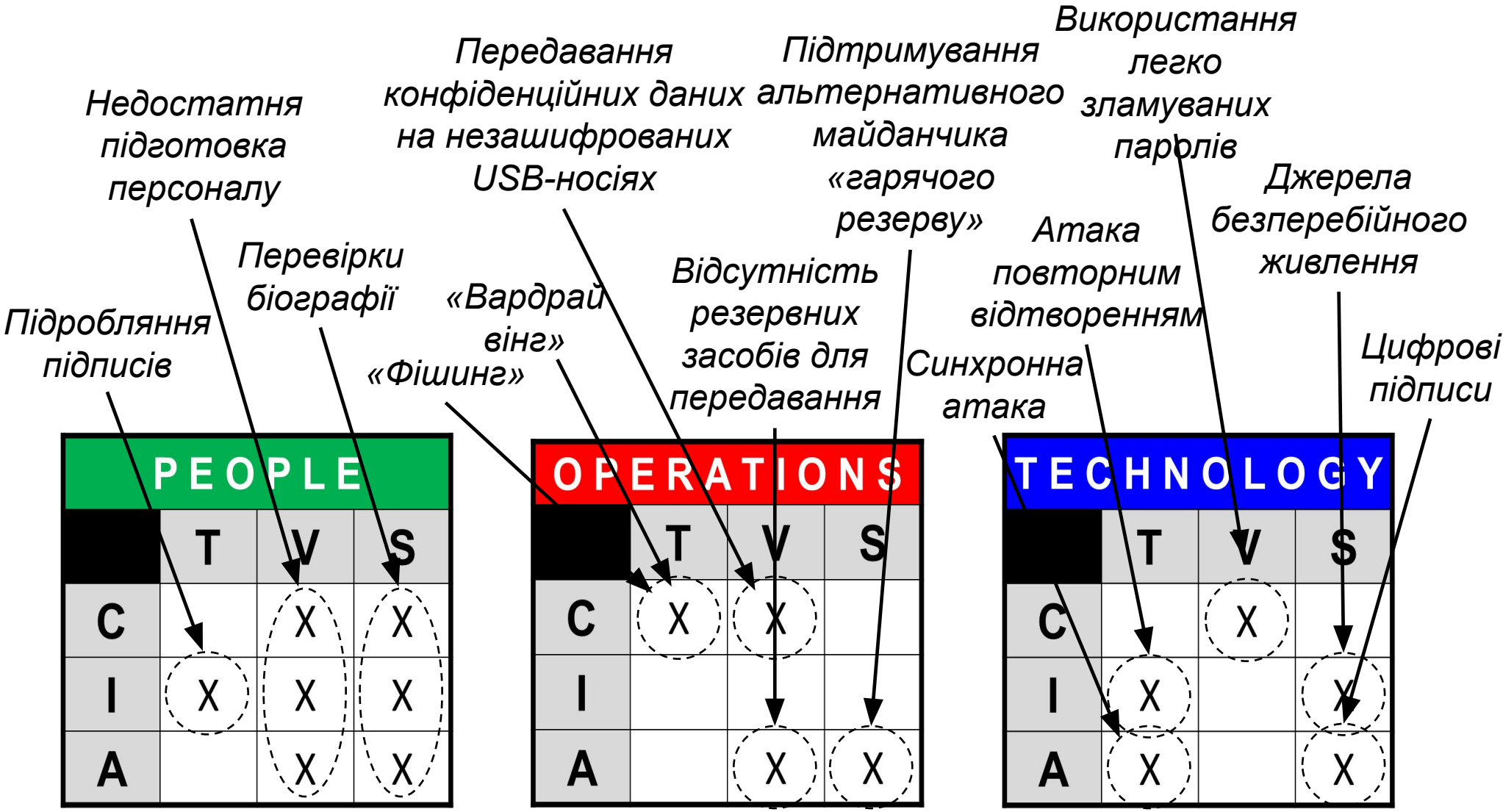
Кіберматриця

Розгляд «тріади CIA» з точки зору людей, операцій і технології і поєднання її з контрольованими параметрами рівняння ризику дає кіберматрицю 3 × 3 × 3. Суть цієї матриці полягає в її можливості широкого охоплення всіх елементів кібербезпеки у зрозумілій формі.

Словами IATFF (Технічний рамковий форум з ІБ)

«По суті організації розв'язують завдання ІБ, доручаючи людям виконувати операції із використанням технології».

Приклади заповнення матриць



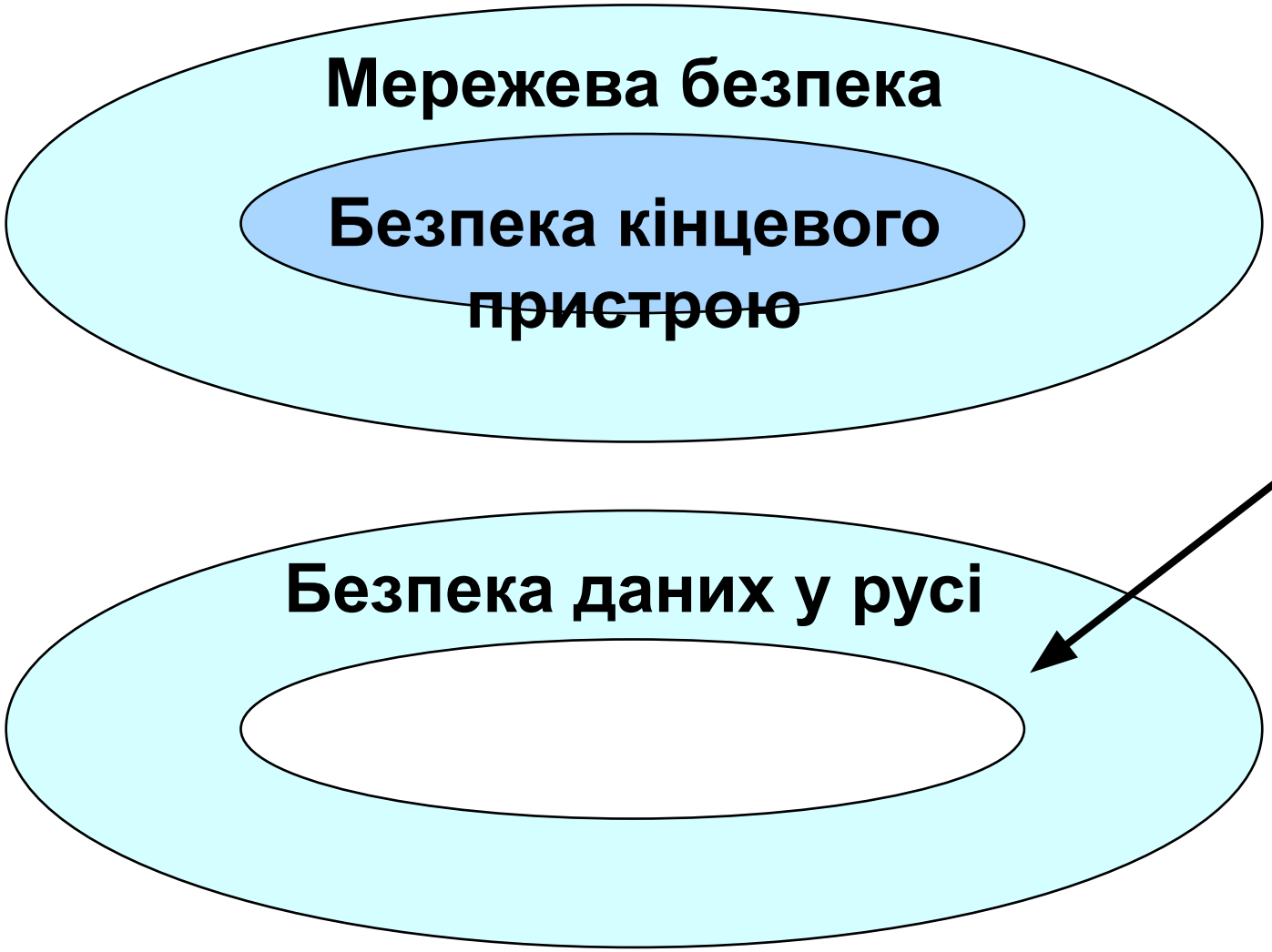
Вразливості

- Їх регулярно виявляють і про них повідомляють:
  - постачальники відповідних пристроїв чи протоколів;
  - організації, що займаються їх пошуком та/або поширенням інформації про них, наприклад:
    - Національна база даних уразливостей
      - nvd.nist.gov
    - MITRE
      - cve.mitre.org
    - Symantec
      - broadcom.com/support/security-center

Заходи з безпеки (загальні)

- Ретельно пропрацьована політика безпеки
- Підготовка й інформування користувачів
- Надлишковість (усунення єдиних точок відмови)
- Встановлення актуальних _____
- Конфігурування для _____ (підказка: Р_ _ Р)
- Регулярне створення резервних копій даних
- Аудит упроваджених механізмів
- Механізми перевірки цілісності
- Механізми контролю доступу

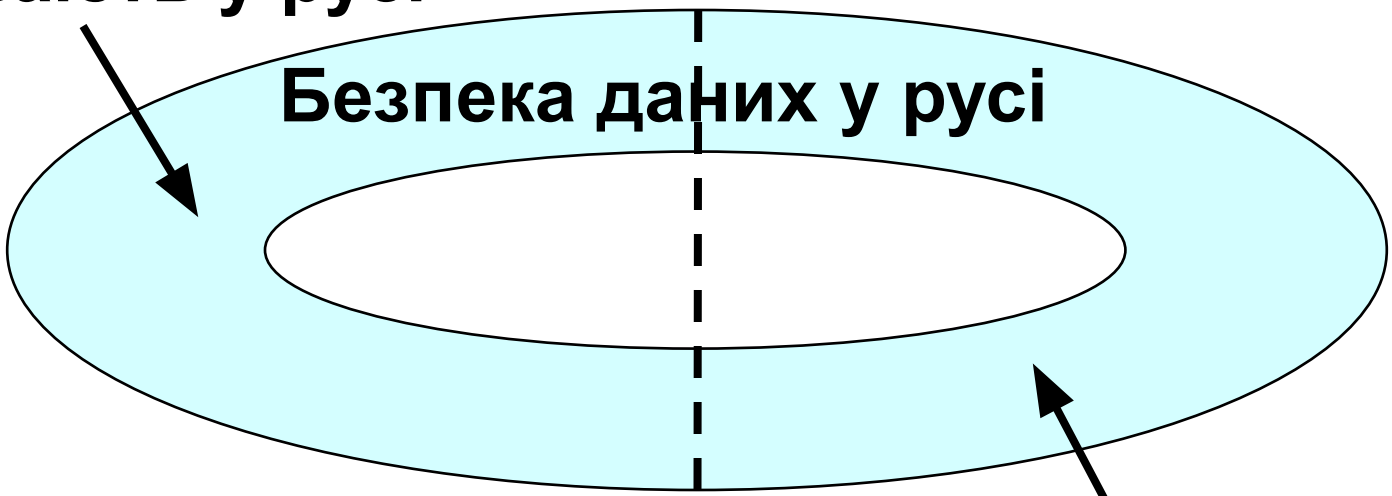
Безпека даних у русі



Якщо можливість виникнення проблем із кінцевим пристроєм усунуто, мережева безпека обмежується аспектами безпеки (тільки) даних у русі

«Хороші» та «погані» дані у русі

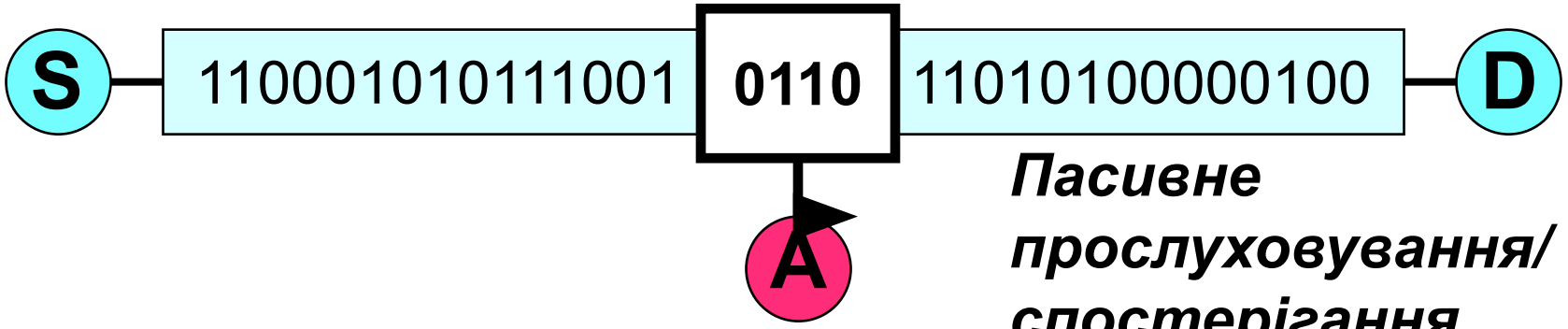
«*Хороші*» дані потрібно захищати, поки вони перебувають у русі



«*Погані*» дані потрібно виявляти та блокувати, поки вони перебувають у русі

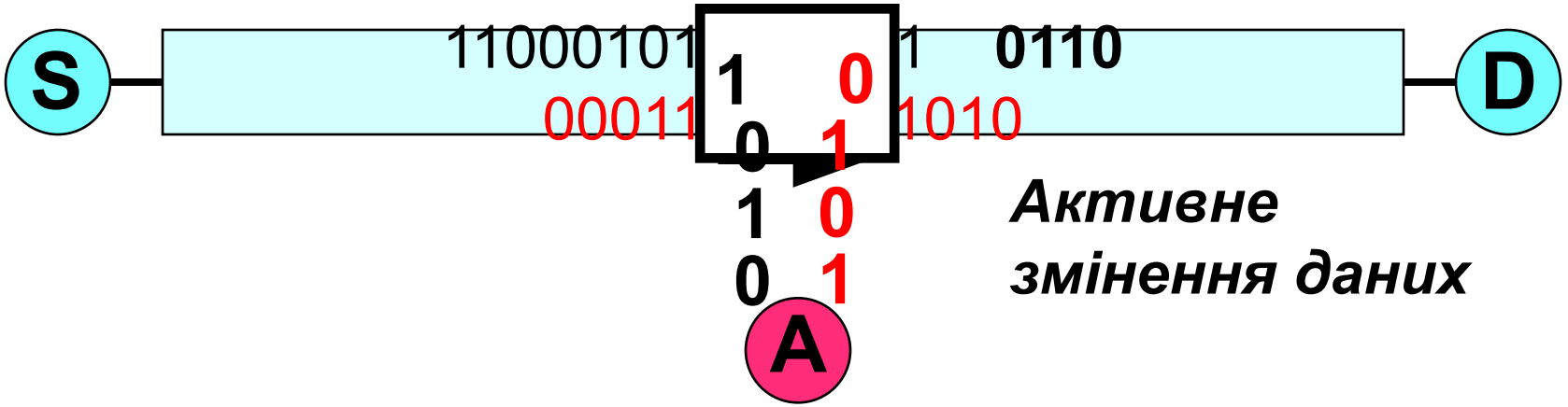
Пасивні й активні атаки

…Міст замінований…



Пасивне прослуховування/ спостерігання

…Міст **безпечний для проходу**…



Активне змінення даних

Загрози для/від бітів у русі

S – достовірне джерело

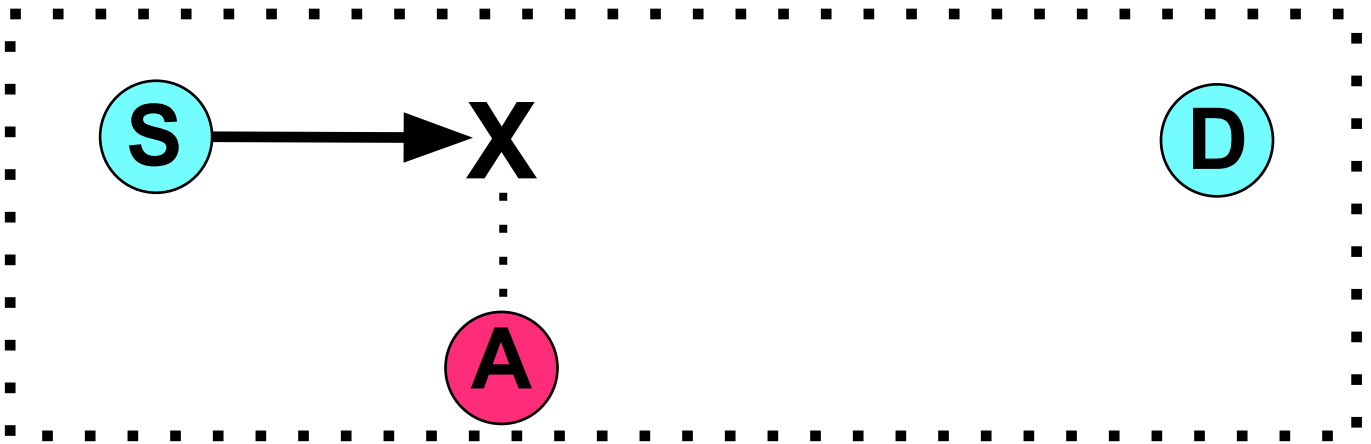
D – достовірне призначення

A – зловмисник

Позначення

Що це?

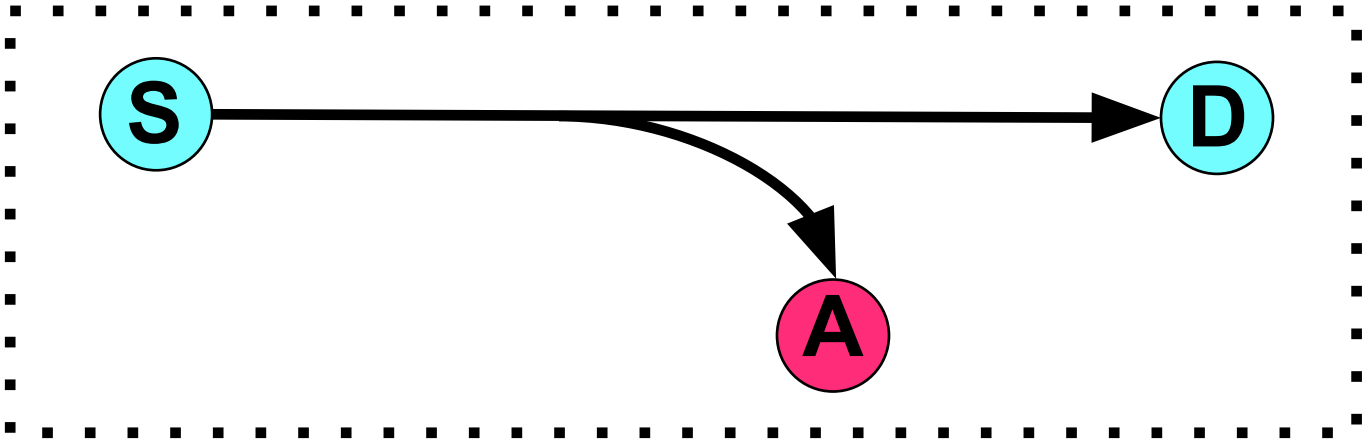
Загрози для/від бітів у русі



Що це?

Атака на

C I A

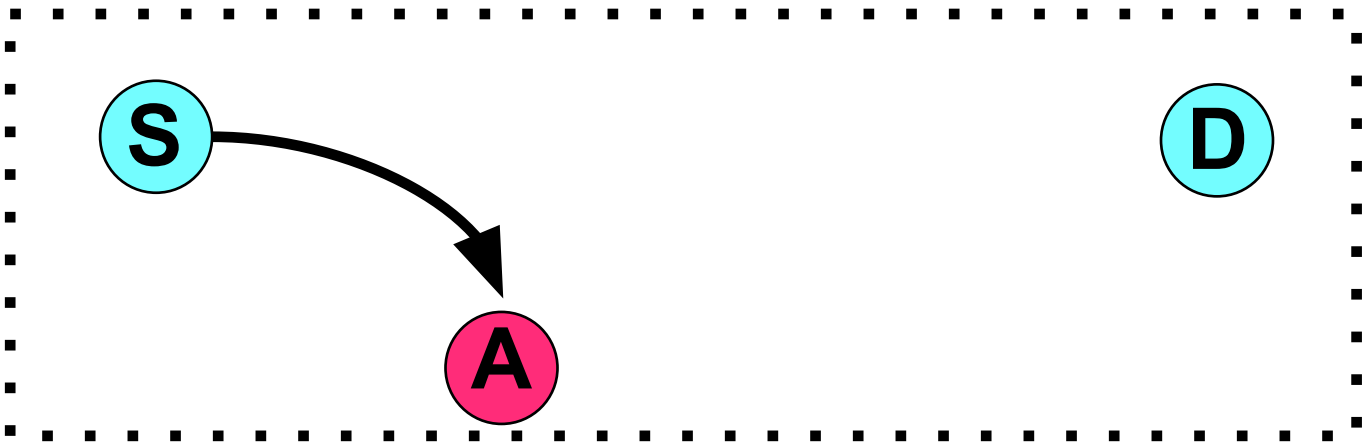


Що це?

Атака на

C I A

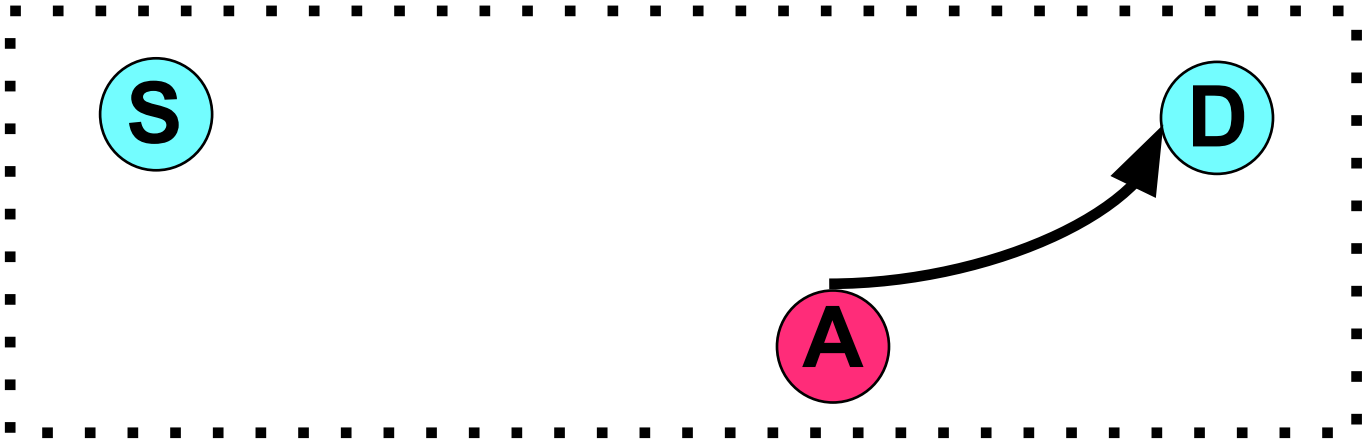
Загрози для/від бітів у русі



Що це?

Атака на

C I A

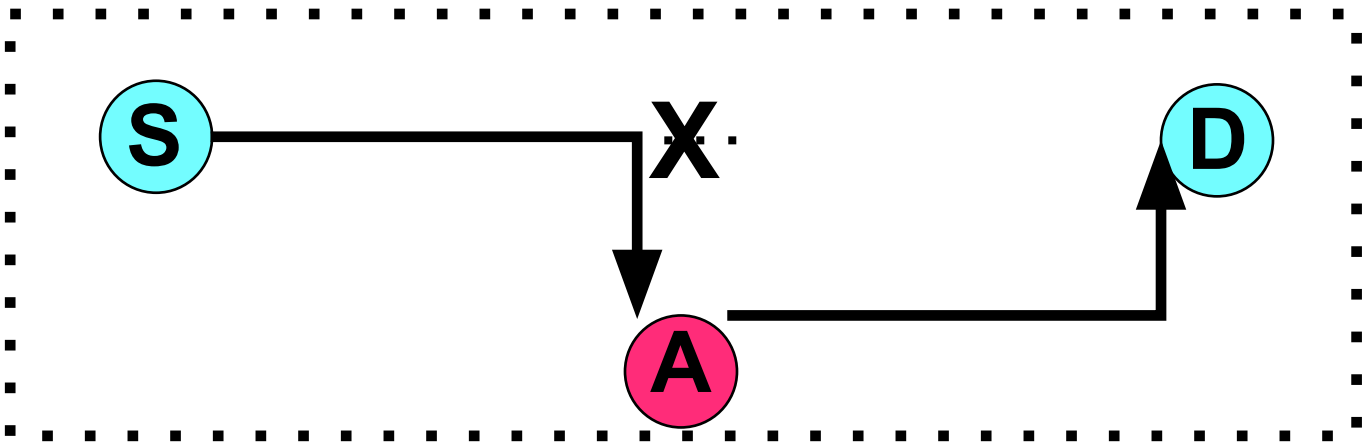


Що це?

Атака на

C I A

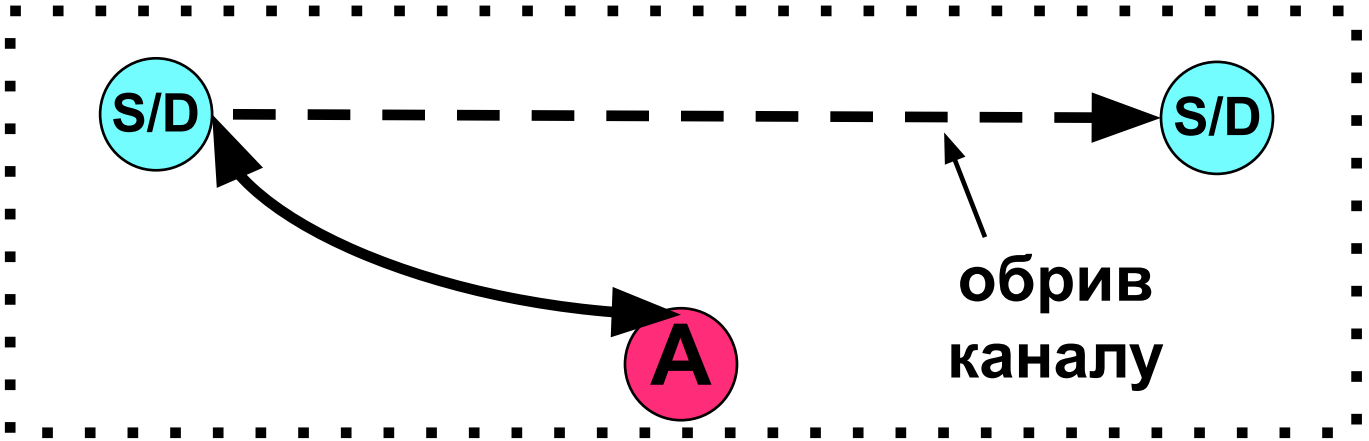
Загрози для/від бітів у русі



Що це?

Атака на

C I A

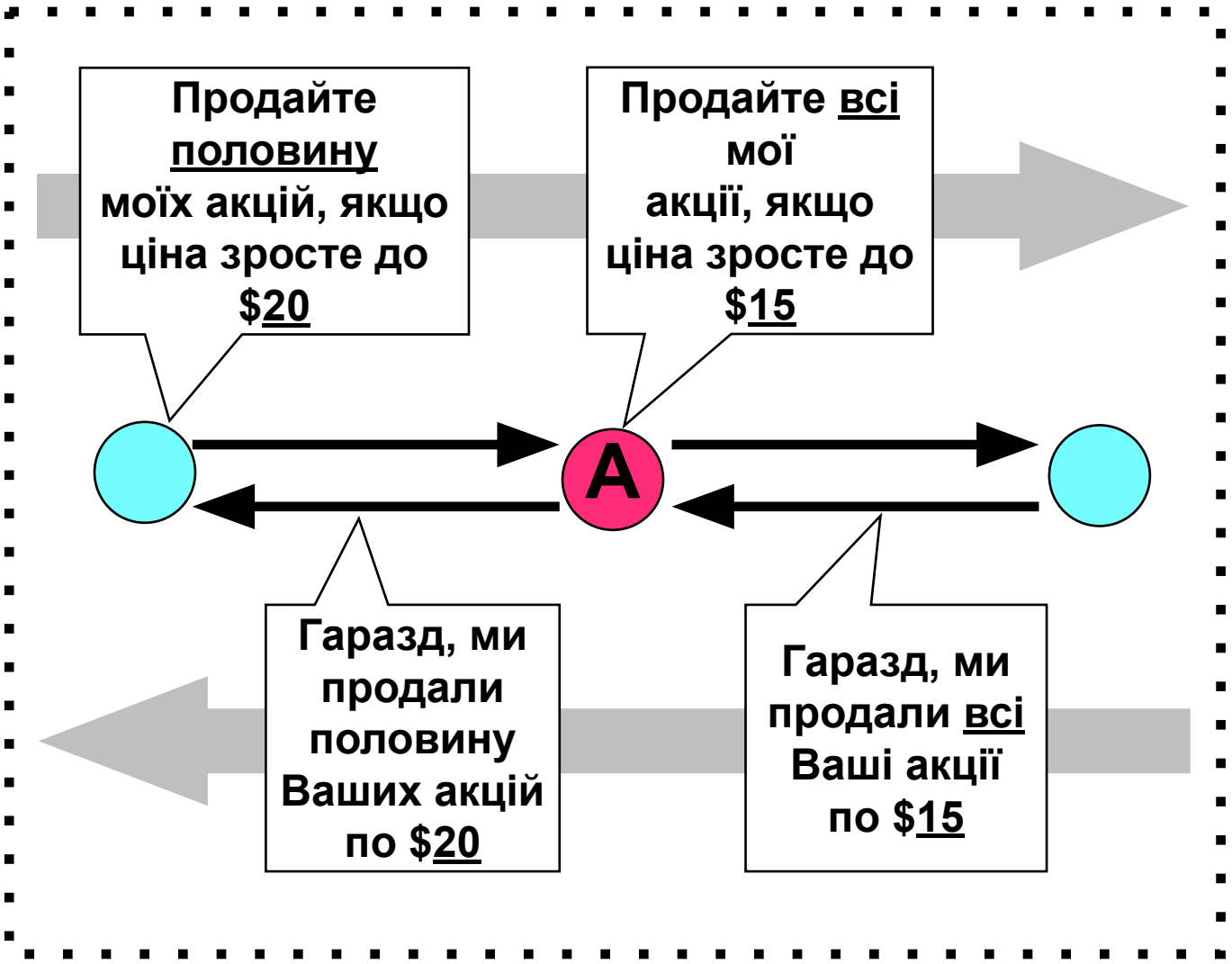


Що це?

Атака на

C I A

Загрози для/від бітів у русі

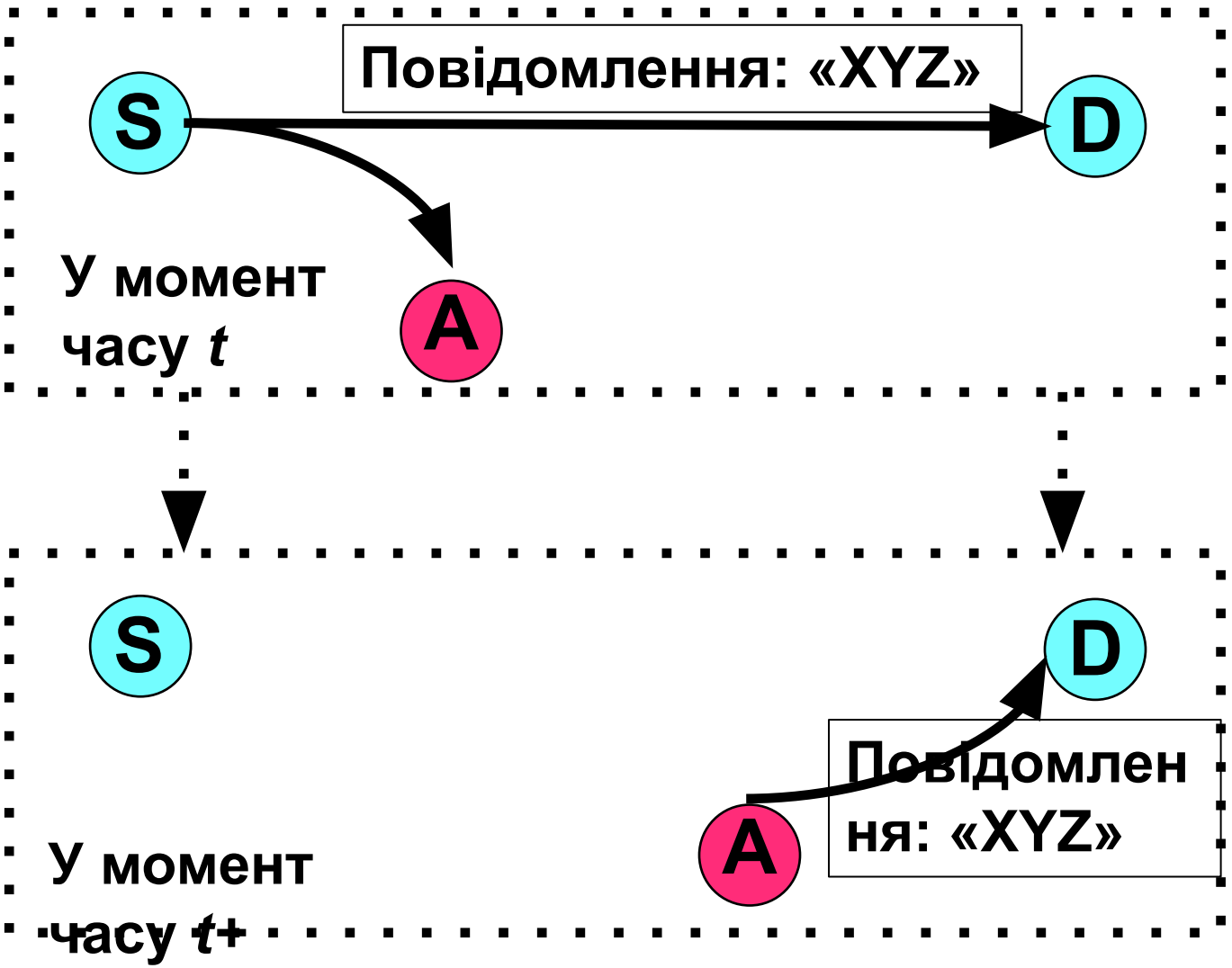


Що це?

Атака на

C I A

Загрози для/від бітів у русі



Нехай «XYZ» захищене шифруванням

Що це?

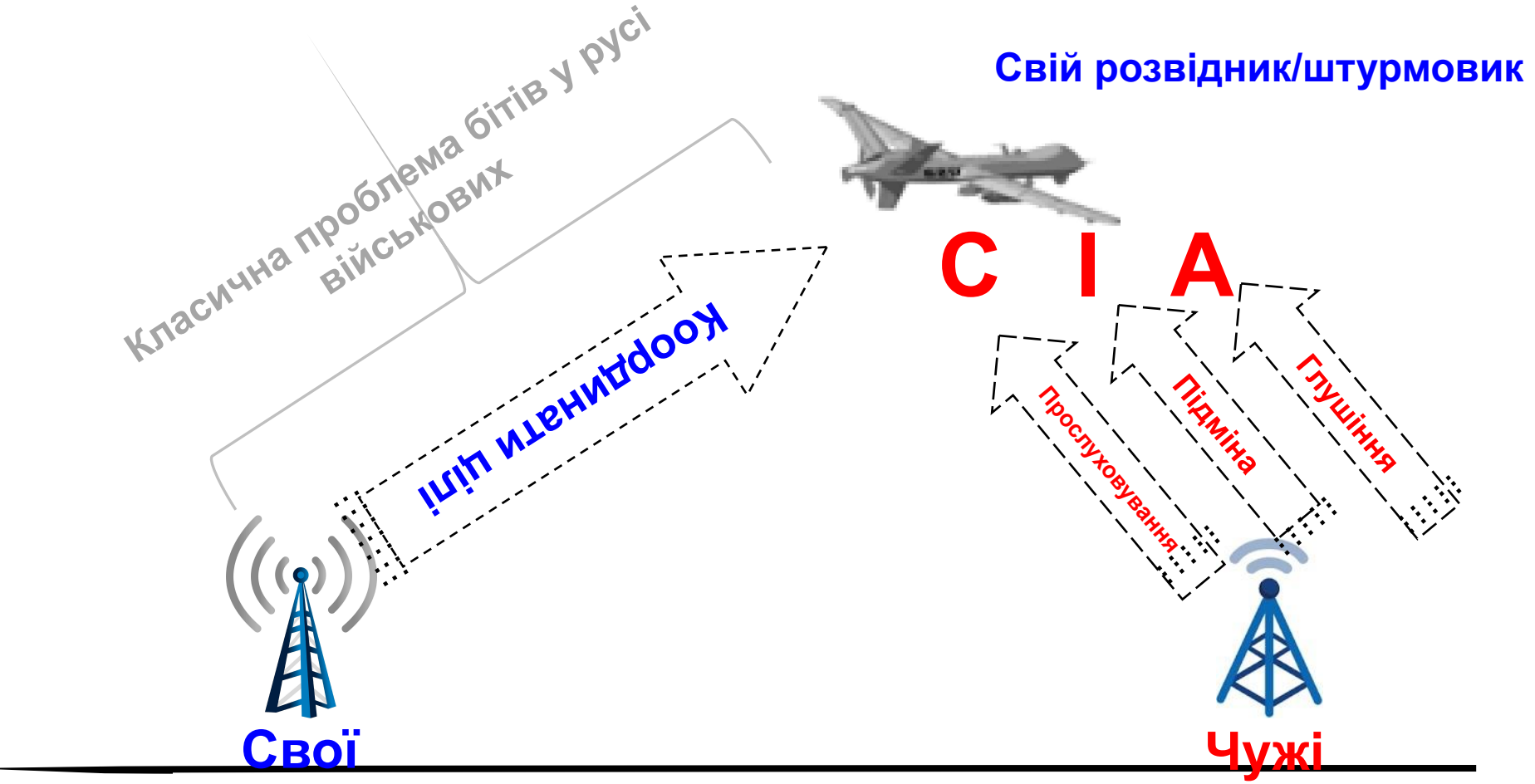
Атака на

C I A

C, I або A?

- **Як би ви розставили пріоритети в тріаді з точки зору зловмисника або захисника?**
- **Відповіді в ключі «це залежить від…» не приймаються.**
- **Розгляньте приклад тактичного сценарію, як на наступному слайді.**
  1. **(Найвища критичність) □ ?**
  2. **(Помірна критичність) □ ?**
  3. **(Найнижча критичність) □ ?**

C, I або A?


Класична проблема бітів у русі військових
Свій розвідник/штурмовик
C I A
Координати цілі
Прослуховування
Підміна
Глушіння
Свої
Чужі

C, I або A?

1. **(Найвища критичність) _____**

   Ворог _____ вашу інформацію!

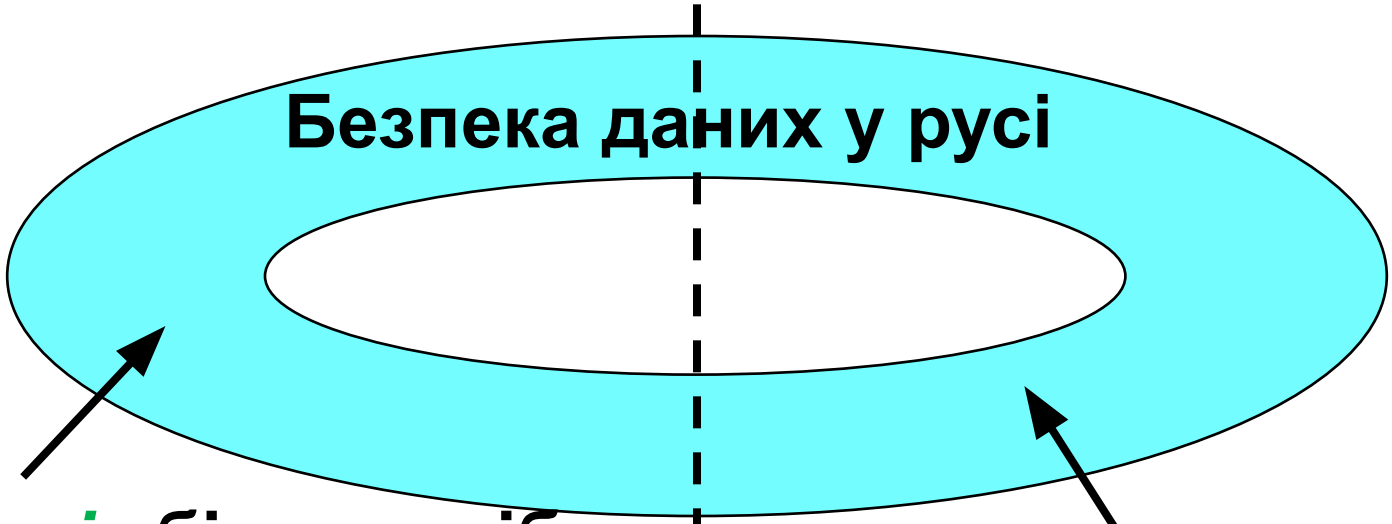
2. **(Помірна критичність) _____**

   Ворог _____ вашу інформацію!

3. **(Найнижча критичність) _____**

   Ворог _____ доступ до вашої інформації

«Хороші» та «погані» дані у русі



«*Хороші*» біти потрібно **захищати**, поки вони перебувають у русі

Рішення: **впровадження криптографічних рішень для забезпечення конфіденційності та цілісності**

«*Погані*» дані потрібно **виявляти** та **блокувати**

Рішення: **Фільтрування… і впровадження автентифікації (через криптографію) з метою виявлення зловмисників**

Групове представлення двійкової інформації та терміни

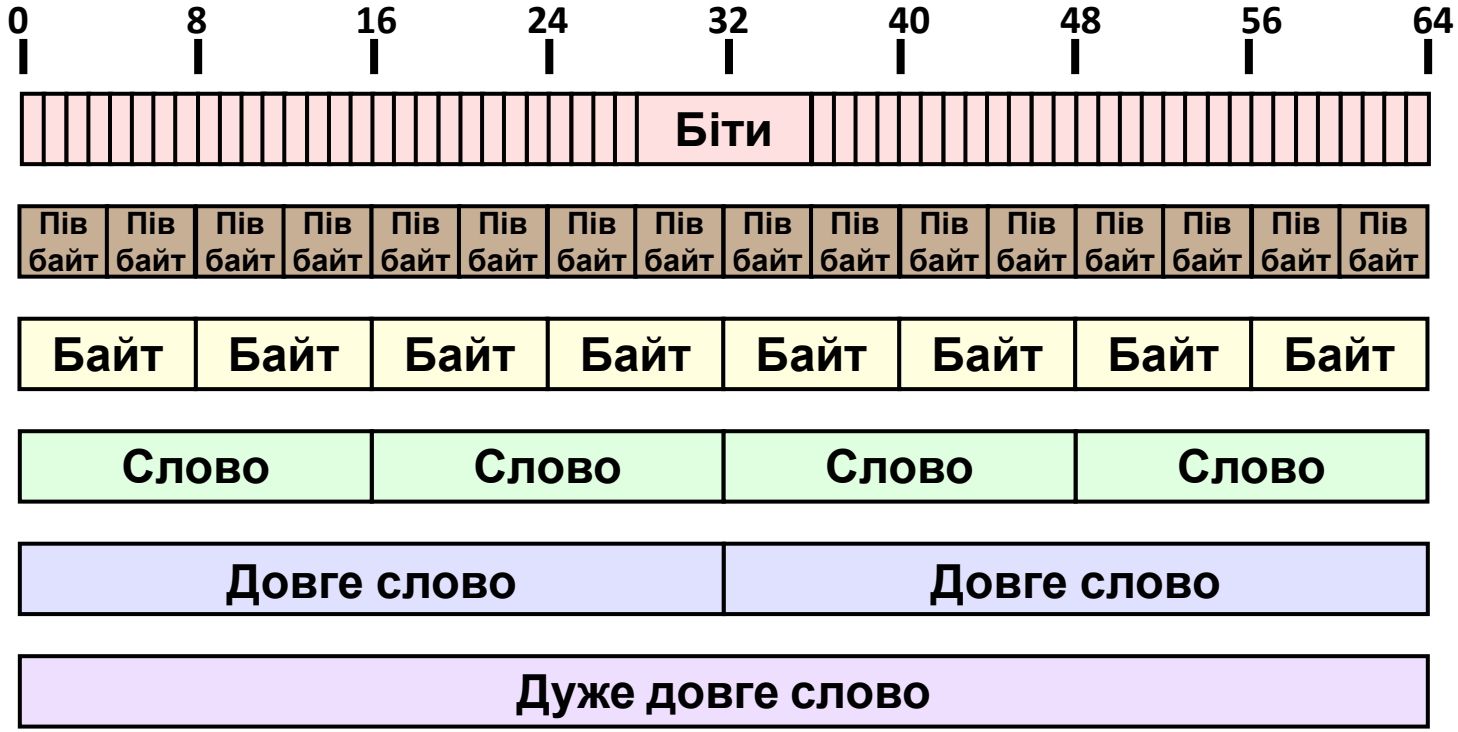
Біт — це двійкове число.

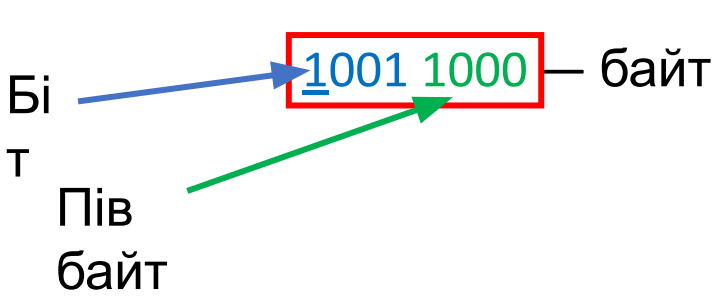
Істинність	Біт
T	1
F	0

Number of Bits	Common Representation Terms
1	Bit / Digit / Flag
4	Nybble / Nibble
8	Byte / Octet / Character
16	Double Byte / Word
32	Double Word / Long Word
64	Very Long Word

Бітовий рядок — це послідовність із нуля чи більше бітів. Довжина такого рядка — це кількість бітів у рядку.

Групове представлення двійкової інформації та терміни

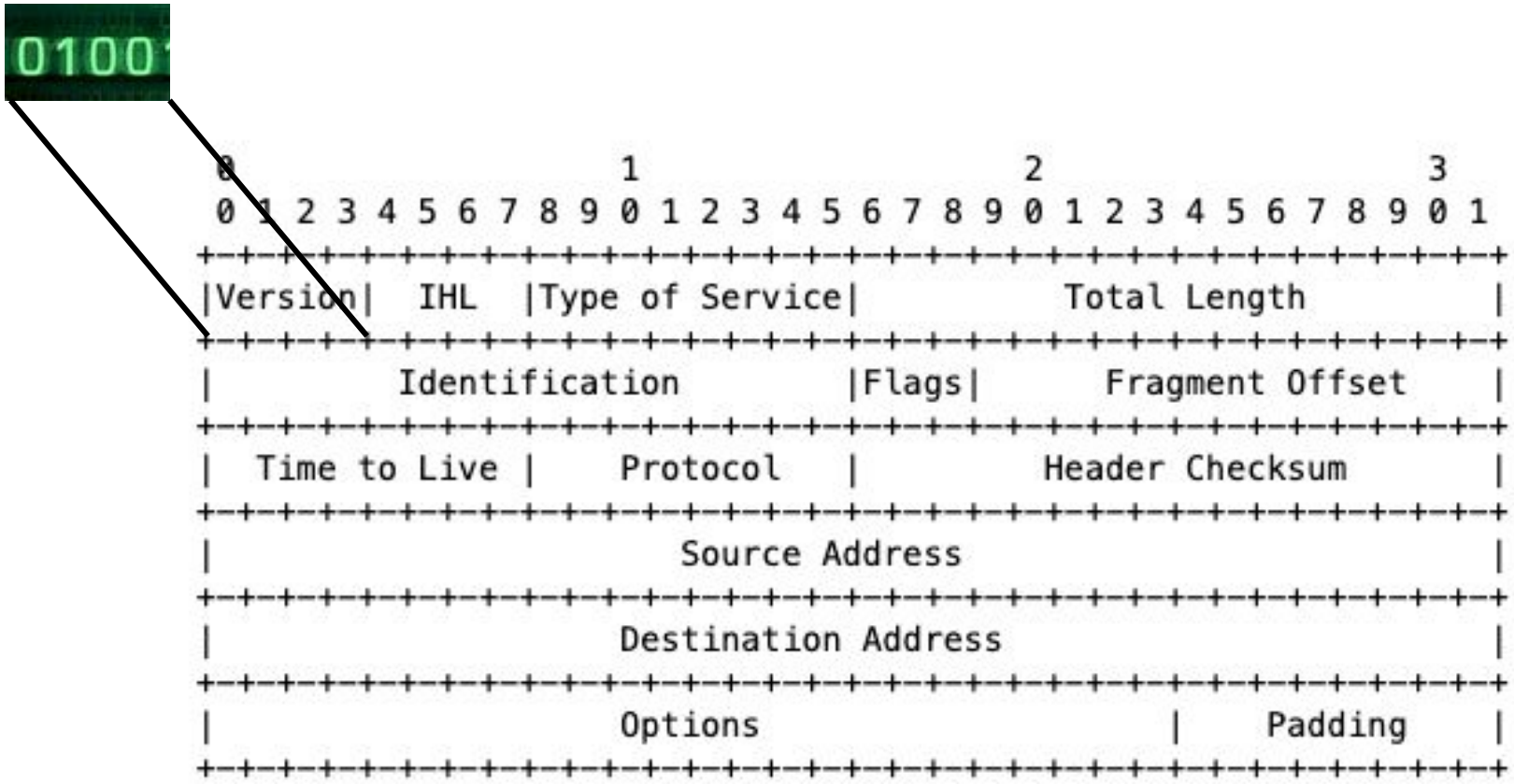




Біт — це двійкове число.

Істинність	Біт
T	1
F	0

Чому це важливо?



Заголовок дейтаграми Інтернет.

Бітовий рядок — це послідовність із нуля чи більше бітів. Довжина такого рядка — це кількість бітів у рядку.

Еквівалентність двійкових і десяткових чисел

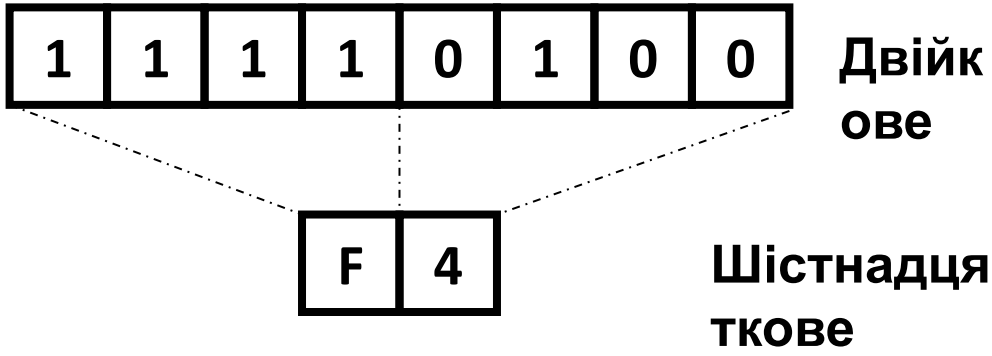
Binary Number	1	1	0	1	0	0	1	1
Power of Two	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Value of Digit Place	128	64	32	16	8	4	2	1
Value For This Number	128	64	0	16	0	0	2	1
Running Sum (from left to right)	128	128+64 = 192	192	192+16 = 208	208	208	208+2 = 210	210+1 = **211**

- **Двійкове число із 8 розрядами може позначати _____ різних значень.**
- **Двійкове число із *N* розрядами може позначати _____ різних значень.**

Еквівалентність двійкових і десяткових чисел

- 101010_2 = _____ у десятковій системі
- 11111100_2 = _____ у десятковій системі
- 128_{10} = _____ у двійковій системі
- 255_{10} = _____ у двійковій системі

Двійкове та шістнадцяткове представлення чисел



- **Двійкові числа незручні для людей і дуже швидко стають надто довгими.**
- **1111 0100 □ (1111)(0100)** ***у шістнадцятковій системі використовуються групи по 4 біти***
- **(1111)(0100) = (15)(4)**
- **F4 у *шістнадцятковій* системі числення, або в системі з *основою 16***

розширення 244_{10} із системи з основою 16

Перетворення двійкових і шістнадцяткових чисел

- **Шістнадцяткове представлення найбільш поширене.**
- **У ньому використовуються групи по чотири розряди.**
- **Компактне представлення двійкової інформації.**
- **Двійкові числа зазвичай представлені групами розрядів у кількості, кратній чотирьом.**

Binary Digits	Octal Digit	Hexadecimal Digit	Decimal Digit
0000	0	0	0
0001	1	1	1
0010	2	2	2
0011	3	3	3
0100	4	4	4
0101	5	5	5
0110	6	6	6
0111	7	7	7
1000		8	8
1001		9	9
1010		A	
1011		B	
1100		C	
1101		D	
1110		E	
1111		F	

Перетворення двійкових, вісімкових і шістнадцяткових чисел

- 0x4D1B = _____ у двійковій системі
- 0x4D1B = _____ у десятковій системі

Перетворення шістнадцяткових чисел на десяткові

Hexadecimal Number	8	3	0	C
Decimal Value of Digit	8	3	0	12
Power of 16	16^3	16^2	16^1	16^0
Value of Digit Place	4096	256	16	1
Value For This Number	4096*8 = 32768	3*256 = 768	0*16 = 0	12*1 = 12
Running Sum (from left to right)	32768	32768+768 = 33536	33536	33536+12 = **33548**

- **0x4D1B = _____ у десятковій системі**
- **(4) (13) (1) (11) □**

  4*16^3 + 13*16^2 + 1*16^1 + 11*16^0 =

  4*4096 + 13*256+ 1*16+11*1 =

  16 384 + 3328 + 16 + 11 = 19 739_{10}

Перетворення десяткових чисел на двійкові

Decimal Value Before Considering This Digit Place	**689**	689	177	177	49	49	17	1	1	1	1
Power of Two	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Value of Digit Place	1024	512	256	128	64	32	16	8	4	2	1
Value of Digit Place Equal To or Less Than Current Decimal Number?	No	Yes	No	Yes	No	Yes	Yes	No	No	No	Yes
Subtraction Step	skip	689- 512 = 177	skip	177- 128 = 49	skip	49-32 = 17	17-16 = 1	skip	skip	skip	1-1 = 0
Binary Digits	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**1**

Перетворення чисел із десяткових на двійкові:найпростіше з трьох перетворення — з десяткових на двійкові, оскільки максимальне значення кожного розряду — одиниця, тож жодного ділення, лише віднімання.

1. **Знаходимо найбільший степінь двох, менший за саме число.**
2. **Ставимо «1» у розряді, який відповідає цьому ступеню двох, і віднімаємо цей ступінь двох від десяткового числа.**
3. **Повторюємо кроки 1 і 2, доки не залишиться нуль.**

689_{10} = _____ у двійковій системі

Перетворення десяткових чисел на шістнадцяткові

Decimal Value Before Considering This Digit Place	689	689	177	1
Power of 16	16^3	16^2	16^1	16^0
Value of Digit Place	4096	256	16	1
Value of Digit Place Smaller Than Current Decimal Number?	No	Yes	Yes	n/a
Division Step	skip	689/256 = 2.691; use “2” for this digit.	177/16 = 11.0625; use “B” for this digit.	n/a
Remainder After Division	skip	177	1	n/a
Hexadecimal Digits	0	2	B	1

Перетворення чисел із десяткових на шістнадцяткові:процес майже такий самий, тільки на степені двох потрібно ділити, а не віднімати їх.

1. **Починаємо з найвищого степеня 16 (шістнадцяткових), який менше числа.**
2. **Ділимо десяткове число на цей степінь і беремо лише цілу частину результату.**
3. **Залишок від ділення залишаємо на наступний крок.**
4. **Повторюємо кроки 1 і 3, доки не дійдемо до розряду одиниць, у який заносимо те, що залишилося після опрацювання старших розрядів.**

689_{10} = _____ у шістнадцятковій системі

Булева логіка та логічні функції

Input #1	Input #2	Output
0	0	0
0	1	0
1	0	0
1	1	1

Таблиця істинності оператора *І*

Input #1	Input #2	Output
0	0	0
0	1	1
1	0	1
1	1	1

Таблиця істинності оператора *АБО*

Input #1	Input #2	Output
0	0	0
0	1	1
1	0	1
1	1	0

Таблиця істинності оператора *виключне АБО* (*XOR*)

Порозрядне маскування (задання)

- Припустимо, в нас є 12-розрядне двійкове вхідне число 101001011010, і нам потрібно задати значення середніх 6 розрядів в одиниці.
- Для цього ми просто застосовуємо до числа 12-розрядну *маску* 000111111000 за допомогою оператора *АБО*.

Input	1	0	1	0	0	1	0	1	1	0	1	0
Mask	0	0	0	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0
Result of OR Operation	1	0	1	**1**	**1**	**1**	**1**	**1**	**1**	0	1	0

Задання розрядів за допомогою бітової маски *АБО*

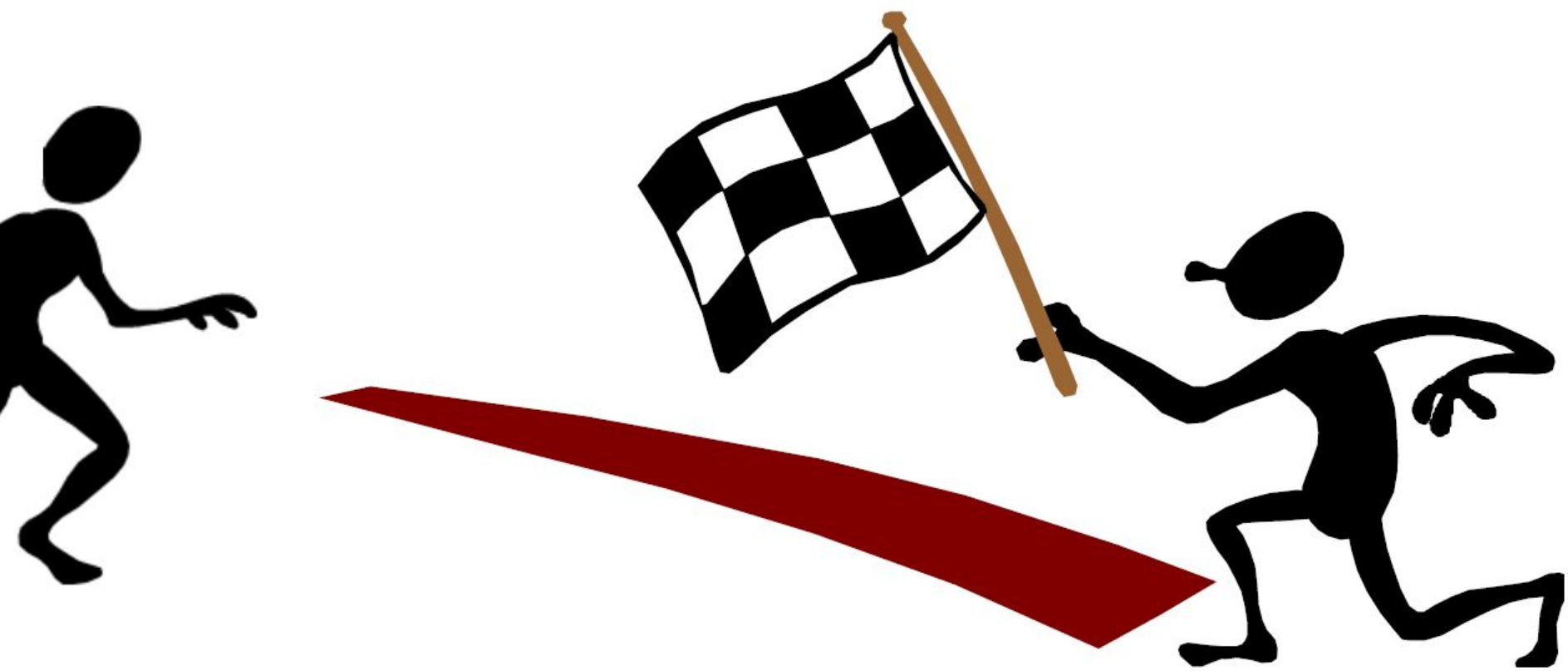
Порозрядне маскування (скидання)

- Припустимо, в нас є 12-розрядне двійкове вхідне число 101001011010, і нам потрібно скинути середні 6 розрядів.
- Для цього ми просто застосовуємо до числа 12-розрядну *маску* 111000000111 за допомогою оператора *I*.

Input	1	0	1	0	0	1	0	1	1	0	1	0
Mask	1	1	1	0	0	0	0	0	0	1	1	1
Result of AND Operation	1	0	1	0	0	0	0	0	0	0	1	0

Скидання бітів за допомогою бітової маски *I*

Кінець



Приклад

- IP-адреса: 192.168.5.5 у десятковому поданні через крапки
- Яке шістнадцяткове представлення?
- Яке двійкове представлення?
- Застосуйте бітову маску 255.255.255.0